CELL PHONE SEARCHES IN A DIGITAL WORLD: BLURRED LINES, NEW REALITIES AND FOURTH AMENDMENT PLURALISM

Steven I. Friedland
**Cell Phone Searches in a Digital World: Blurred Lines, New Realities and Fourth Amendment Pluralism**

“Look at that chair, we understand it because its form and function are the same thing, which is how the manufactured world has been for hundreds of years, ... And then incredibly and relatively recently, there’s this opportunity but with a set of problems to create objects whose forms don’t hint at what they do. And they’re packed with incredible sophistication and capability.” -- Jony Ive, the Apple designer behind the iMacs and iPod.1

October 15, 2013

S. Friedland

**Abstract:** State and federal courts are split over whether cell phone searches incident to a lawful arrest are permissible under the Fourth Amendment. The Supreme Court has the opportunity to create uniformity by accepting a certiorari petition in a cell phone search incident to arrest case, either United States v. Wurie or Riley v. California. The Court should do so to create an analysis that incorporates sensory enhancing technology, not avoids it, as it has done to date.

The split in case law evidences a central contradiction. Fourth Amendment rules need to be predictable and based on clear guidelines for effective and safe crime interdiction. Technological advances cloud the application of the rules by introducing new facts into the calculus, facts that separate form from function and transform the analysis. In the past, as evidenced by search cases Katz and Jones, and exception cases for searches incident to lawful arrest, Chimel and Robinson, the Supreme Court analysis tended to be based on abstract and grand theory, which has led to a form of Gresham’s Law of constitutional application, where general principles often end up marginalizing specific provisions. Because of advancing technology, however, Fourth Amendment protection has been eroding, as predicted in Kyllo. Searches of cell phones incident to lawful arrests can provide a huge source of discretionary information for police, and searches of "smart" phones without cause can seem like a fishing expedition. Comparisons and analogues have not worked. Neutral narratives have been fractured and unsatisfying.

This paper suggests using local structures accommodating post-digital technology instead of pre-digital comparisons like containers and walls and doors. Facts, and new realities, matter. In essence, analyses should incorporate the capabilities of the technology in question. The new doors and walls of the advancing technology era create new privacy encroachments, including nondiscoverable information without permission, but are still guided by the same textual and Framers’ intent considerations, such as invasiveness, duration and intent of the government conduct, as well as the nature and impact of the invasion. In light of this calculus, cell phone searches incident to a lawful arrest generally should require some sort of independent

---

and legitimate reason to search the device, a search of which does not fit neatly into existing rationales of container, officer safety, or destruction of evidence.

***************

I. Introduction

State and federal courts are split on whether cell phone searches incident to a lawful arrest are permissible under the Fourth Amendment. The Supreme Court has the opportunity to review a cell phone search case in its 2013-2014 term, either the First Circuit case, United States v. Wurie, or the state court case, California v. Riley. Wurie involved a police search of a cellular phone’s face plate and of the telephone number of a person who had just called the phone, along with an associated name for the number. Riley involved the search of a “smart” phone by police officers, who searched and located some incriminating texts on the phone.

The current split in cases evidences a central contradiction. Fourth Amendment exceptions need predictability and clarity to guide the relationship between the public and government agents engaged in crime interdiction. Technological advances, on the other hand, cloud the application of the rules by separating form from function and introducing new facts into the calculus that transform pre-digital understandings and the resulting legal analysis. In the past, as evidenced by cases such as Katz v. United States, Chimel v. California and United States v. Jones, the Supreme Court has tended to eschew considering the particular sensory enhancing technology involved and its impact on physical reality in determining whether the use of the technology constituted an unlawful search. Instead, the Supreme Court analysis tended to be based on the pre-digital world of general or grand theory, with physical walls and doors, even including a phone booth’s walls. The reasonable expectation of privacy test, advanced in Justice Harlan’s concurrence in Katz, as well

---

2 Amendment IV, United States Constitution.
3 ___ F.3d ___ (1st Cir. 2013).
4 Riley, 2013 WL 475232.
5 See, e.g., Orin Kerr, "Foreword: Accounting for Technological Change," 36 Harv. J. of Law and Pub. Pol. 403 (2013) ("A law created for one world may have a very different impact when applied to the facts of a different era. As a result, changing technology and social practice often trigger a need for legal adaptation.").
7 395 U.S. 752 (1969)(setting forth the “wingspan” test for searches incident to lawful arrest).
8 565 US. ___ (2012).
9 One major exception to this proposition is Kyllo v. United States., 533 U.S. 27 (2001).
10 Utilizing a Gresham’s Law of constitutional application, general principles often end up marginalizing specific provisions.
as the bright lines of the Chimel “wingspan” test and the Jones trespass test, work well in a world configured by solid doors and walls. Unfortunately, the new technologies simply do not fit neatly within the bright line categories, creating different types of doors and walls through encryption, Trojans and other invisible intruders. Because of advancing technology, Fourth Amendment protection has been eroding, as foreshadowed in Kyllo v. United States. Searches incident to lawful arrest of cell phones provide a huge source of discretionary information for police and investigators, who will continue to seek advantage and efficiency through technology. Comparisons and analogues have not worked. Neutral narratives have been fractured and unsatisfying.

This paper suggests that the preferable solution for cell phone searches incident to arrest is to view cell phones as portals to information, past, present and future, requiring presumptive privacy protection. This approach uses local structures instead of grand theory and is grounded on the new realities presented by the technology in question, not an analogue from the pre-digital technology world of physical doors and walls. In doing so, it should first be recognized that the technology is fact-changing and transformative and second, that significant technology change will impact Fourth Amendment analysis. Third, the courts should incorporate new technological realities into a pluralistic approach, such that the nature of digital phone technology, if part of the facts, is relevant to assessing whether cell phone searches fall within the searches incident to lawful arrest exception.

Building on Kyllo and Carney v. California, guidance to lower courts and criminal investigators alike should be consistent with the text and history of the Fourth Amendment. Courts should consider: (1) the invasiveness, duration and intent of

---

11 Even the telephone booth in Katz had solid walls creating a “private” space.
12 533 US. 27 (2001)(involving the unconstitutional use of a thermal imaging device by the police to detect heat emanating from a private residence).
13 The word “reasonable” in the Fourth Amendment is an indication that local structures contemplated.
14 Essentially, circumstances matter. There are rationales that justify searches - false compartment? Is there a phone bomb? Is the phone dialing or “pinging”? However, the general presumption is that a “smart” or cellular phone is not subject to the SILA rationale.
16 Otherwise, government will find backdoors and use invisible intercepts to undermine privacy without the subject necessarily even knowing about the presence of an intruder. The new doors and walls of the advancing technology era likely involve privacy encroachments, including accessing nondiscoverable information without permission, but are guided by the same textual and Framers’ intent considerations.
17 By including intent, the test limits government discretion to engage in invasive tactics. Even the Third Amendment on quartering soldiers reflects that idea.
the government conduct; and (2) the nature, exposure and impact of the invasion.\textsuperscript{18}

The requirement of at least a legitimate and articulable basis is consistent with \textit{Kyllo}, and, on a broader scale, with maintaining a public/private distinction within our open democracy.

The paper has four parts. After this Introduction, Part II explores the basic doctrine for searches and seizures, including the exception for searches and seizures incident to a lawful arrest. Part III then discusses advancing technologies relevant to cellular telephones, and shows why existing analogies based on pre-digital physical reality generally fail. Part IV utilizes local structures to construct predictive and relevant standards for assessing the constitutionality of a search incident to a lawful arrest consistent with the text and intent of the Fourth Amendment.

II. Basic Fourth Amendment Search and Exception Doctrine

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons to be seized.\textsuperscript{19} – the Fourth Amendment

The text of the Fourth Amendment indicates it protects against government searches and seizures without a properly obtained warrant and against otherwise unreasonable searches and seizures. In essence, even if the police do not obtain a warrant, the search must be reasonable in light of privacy interests. One established exception involves searches of arrestees incident to a lawful arrest, which will be discussed in greater detail later in this section.

\textbf{A. Origins of the Fourth Amendment}

The text and history of the Fourth Amendment are a common starting point for most interpretive analyses. The Fourth Amendment was adopted largely in response to the existence of British writs of assistance and general warrants that permitted British constables considerable latitude in searching people’s houses, including their private papers and things.\textsuperscript{20} The adoption of the Fourth Amendment appeared to be

\textsuperscript{18} In light of the new realities and the stated rationales for searches incident to arrest, searches of cellular “smart” phones incident to lawful arrests generally should be considered privacy encroachments, requiring some legitimate and articulable reason for the search.

\textsuperscript{19} Amendment IV, United States Constitution.

a direct attempt to limit search and seizure power by circumscribing unfettered
government discretion. According to commentators, “These principles arose from
the harsh experience of householders having their doors hammered open by
magistrates and writ-bearing agents of the crown….With few exceptions, the
searcher was free to look anywhere and seize anything.”

1. Entick v. Carrington

Entick v Carrington, a 1764 case arising out of an alleged libel in a newspaper
published in North Briton is often cited to illustrate the rationale for the adoption of
the Fourth Amendment. In particular, Entick describes the strong reaction against
writs of assistance or general search warrants that were common in Seventeenth-
Century England, providing the constable with extensive discretion to search and
seize. By the 1760s, general warrants had little technical grounding, and their use
had experienced a decline in most areas outside of newspaper regulation and
seditious libel. The general warrants were still used, though, based on long-
standing custom. The alleged libel in the North Briton newspaper controversy
spawned several privacy-related cases, including Entick, where a writ of assistance
was signed to search Entick’s house for evidence of the libel. When the search
concluded unsuccessfully, Entick sued, claiming his rights had been violated.
Entick’s counsel argued against allowing such discretionary, unbounded searches,
claiming they:

would be worse than the Spanish inquisition; for ransacking a man’s
secret drawers and boxes, to come at evidence against him, is like
racking his body to come at his secret thoughts. The warrant is to seize
all the plaintiff’s books and papers without exception, and carry them

22 Id.
23 Even the Supreme Court noted: “Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765), is a “case we have described as a ‘monument of English freedom’
’undoubtedly familiar’ to ‘every American statesman at the time the Constitution
was adopted, and considered to be ‘the true and ultimate expression of
constitutional law”’ with regard to search and seizure.” Brower v. County of Inyo, 489 U.S. 593, 596 (1989)(quoting Boyd v. United States, 116 U.S. 616, 626 (1886)).
24 The writs of assistance experienced their heyday in the reign of King James I, in the early 1600s. Historical Antecedents of the Constitutional Right to Privacy, 2 Dayton L. Rev. 157, 165 (1977); N. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 25 (1937).
25 Id. “Historical Antecedents of the Constitutional Right to Privacy,” 2 Dayton L. Rev. at 167.
before Lord Halifax. What? Has a Secretary of State a right to see all a man’s private letters of correspondence, family concerns, trade and business? This would be monstrous indeed; and if it were lawful, no man could endure to live in this country.27

Lord Chief Justice Camden agreed that the time had come to cease giving the sovereign such unchecked power:

[I]f the point should be determined in favour of the jurisdiction, the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger ...28

The Court added:

This case was compared to that of stolen goods; Lord Coke denied the lawfulness of granting warrants to search for stolen goods, 4 Inst. 176, 177, though now it prevails to be law; but in that case the justice and the informer must proceed with great caution; there must be an oath that the party has had his goods stolen, and has strong reason to believe they are concealed in such a place; but if the goods are not found there, he is a trespasser ....29

C. Further Defining a Search

What constitutes a search in the past several decades has revolved around the subjective and reasonable expectation of privacy test30 as set forth in Katz v. United States.31 In finding that a public phone booth could provide protection under the Fourth Amendment, Justice Harlan’s concurrence provided a standard for future decisions -- the occurrence of a search depended on both a person’s subjective expectations and society’s reasonable expectations of privacy. What a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”32 That which is knowingly exposed to the public, on the

27 19 How. St. Tr. at 1038.
28 19 How. St. Tr. at ____.
29 19 How. St. Tri. at 818.
30 The test has been simplified and characterized as follows: “Rather, even in the absence of a trespass, “a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” Id., at 33; see also Smith v. Maryland, 442 U. S. 735, 740–741 (1979); Katz v. United States, 389 U. S. 347, 361 (1967) (Harlan, J., concurring). Sotomayor, J., Concurring, United States v. Jones, ___ U.S. at ___ (2012).
31 See Katz, 389 U.S 347.
32 Id. at 351.
other hand, what has become known as the “third party rule,” does not qualify for privacy protection under the Fourth Amendment.\(^{33}\)

*Katz* was an advanced and adaptive case for its time, especially when compared to established law.\(^{34}\) While the *Katz* privacy concept was elastic—about people, not places—and included an assessment of context, as a spatial matter, it is still anchored to physical place dimensions.\(^{35}\) Unreasonable searches and seizures were easier to identify in an age dominated by physical action—police stakeouts,\(^{36}\) for example, or eavesdroppers lurking in shadows. While physical surveillance could be extremely revealing, gaps would necessarily occur, as well as human error.

Perhaps the *Katz* progeny that has the most relevance today to the disclosure of electronic data from cellular phones and other devices is *Smith v. Maryland*,\(^{38}\) despite in 1979. Despite being decided more than thirty years ago, a lifetime in technological development, *Smith* has been the gatekeeper of much electronic information. *Smith* involved a pen register that identified the phone calls made on a particular telephone. The telephone numbers called on Smith’s phone indicated he

\(^{33}\) *United States v. Miller*, 425 U.S. 435 (1976), involving government access to bank records, has turned out to be a key case for its potential as an analogue. The defendant moved to suppress a government subpoena for microfiche of his checks and deposit records, claiming they were protected under the Fourth Amendment. The trial court denied the motion, but the Court of Appeals reversed. The Supreme Court held that the government under the Fourth Amendment did not illegally seize Miller’s bank records because such records were not imbued with a reasonable expectation of privacy because they were used by and exposed to bank employees in the ordinary course of business. Without Fourth Amendment protection, a third party can be the subject of a government subpoena to turn over records it is holding, even if the request is part of a criminal investigation.

\(^{34}\) See, e.g., *Olmstead v. United States*, 277 U.S. 438 (1928).

\(^{35}\) Conceptually, there still existed useful boundaries, even in a phone booth like Katz’s, such as walls, doors and windows. These boundaries provided bright lines for what was reasonably expected to lie outside of the government’s purview.

\(^{36}\) It is much more difficult to define and maintain freedom from government and private intrusion, essentially with aggregated public information and words once sent not subject to ready recall. An all-or-nothing definition of privacy no longer is functional. Information travels, is stored with various companies, and is accessible by many. Information has great value, from biometrics, to DNA, to social security and credit card numbers.

\(^{37}\) The film, *Stakeout* (Touchstone Pictures 1987), illustrates what kind of dedicated physical presence was needed to catch criminals in the act. While such surveillance locations are still in use, technology has changed in many ways how police work occurs.

\(^{38}\) 442 U.S. 735 (1979).
was involved in unlawful betting activity. Smith moved to suppress the evidence of the pen register in violation of his Fourth Amendment rights. The Supreme Court found that the telephone numbers – much like metadata today – were disclosed to the phone companies and not within the reasonable expectations of privacy under *Katz*. Therefore, the numbers were wholly without constitutional protection from the government.  

What *Smith* did was open up a wide swath of aggregated information to public access and analysis. Telephone metadata was exempted from constitutional protection as was various computer-related metadata. This burgeoning category included domestic call records, IP addresses, subscriber information, and cell site historical location information. This information would be valuable to several constituencies, from advertisers and retailers, to government data bases, to criminals.

Specifically, *Smith* allowed billions of data sets to be stored and then analyzed by the government without any constitutional limit. In practical terms, the National Security Agency alone takes in 20 billion record events daily. This is significant on many levels. Metadata offers both government and private sleuths opportunities not found in the predigital world – easy to analyze data using software programs and not human labor, which is much more efficient and accurate. The massive expansion

39 Of course, Congress has provided some statutory privacy protection, but this protection has many gaps and is not based on the same high standards as applied under the Fourth Amendment. See the Electronic Communications Protection Act (ECPA), 1986, for example. Recent advances, such as "cloud" storage of electronic data, also are not as protected under the law, which has not kept up with technology and culture.

40 Cf. *United States v. Warshak*, F.3d 266 (6th Cir. 2010).

41 Note that even domestic phone calls can be accessed as part of the government’s terror interdiction efforts. In a recent Foreign Intelligence Surveillance Court Order released on September 20, 2013, the Court found that domestic calls are relevant under §215 of the Foreign Intelligence Surveillance Act (FISA) because:

"Individuals associated with international terrorist organizations use telephonic systems to communicate" and because the government argued that bulk collection is "necessary to create a historical repository of metadata in order to identify known and unknown operatives." *Id.*

42 While some limits were set by the Stored Communications Act and other statutes, these laws are widely considered weak and inefficient.

of data storage is matched only by the increase in scope of digital histories – a generally more detailed replacement for investigative dossiers. Further, encryption tools that protect the data can be more readily compromised when it comes to metadata than hardware and other forms of information.

While the information within messages, such as email and texts, have been protected, the disclosure of the metadata has provided a plethora of clues about what the contents of the messages are. For example, if a person is writing a urologist, it provides inferences about the contents of any communications that might occur.

In addition to the reasonable expectation of privacy test supplied by Katz, Fourth Amendment search doctrine also included trespasses onto private property. The trespass doctrine owes its origins to cases like Entick, as well as Olmsted v. United States. In Olmsted v. United States, the Supreme Court found that the Fourth Amendment does not protect telephone wires from a home to the outside world. The Court found that the wiretapping was not a violation of the Fourth Amendment because there was no actual “entry of the houses or offices of the defendants.”

Olmstead essentially offered a property and tort law analysis of trespass in defining the scope of the Fourth Amendment.

In Jones, the Court found a violation of Mr. Jones’s Fourth Amendment rights when the police used a Global Positioning System (GPS) device in 2005 to track his auto in public continuously for 28 days (four weeks). While the government had obtained a warrant for the tracking device, believing that Jones was engaged in narcotics trafficking, the time within which to install it on Jones’s Jeep Grand Cherokee had expired. The government obtained more than 2,000 pages of information from the GPS tracking device affixed to Jones’s car, which was accurate to 50 to 100 feet.

Justice Scalia was careful to point out that Katz did not replace existing trespass doctrine: “But as we have discussed, the Katz reasonable-expectation-of-privacy test

---

44 Olmsted v. United States, 277 U.S. 438 (1928). Olmsted has been routinely cited for providing a traditional and sweeping test of a Fourth Amendment search intersecting with notions of private property, namely the idea of a right to exclude others from accessing the property, including the government, without permission.
45 277 U.S. 438 (1928).
46 Id. at 464.
47 Interestingly, as the Supreme Court points out, the Jeep was not Jones’s, but rather was registered to Jones’s wife. Even so, it was not contested that Jones was “the exclusive driver” of the car and therefore had proprietary interest in it, enough to have standing to move to suppress the GPS tracking data. Jones, 565 U.S. at N. 2 (2012) (Justice Scalia also noted in the footnote, “If Jones was not the owner he had at least the property rights of a bailee. The Court of Appeals concluded that the vehicle’s registration did not affect his ability to make a Fourth Amendment objection, ibid, and the Government has not challenged that determination here. We therefore do not consider the Fourth Amendment significance of Jones’s status.” Id.)
has been added to, not substituted for, the common-law trespassory test.”48 Yet, Justice Scalia had the opportunity to clarify the rules going forward relating to advancing technology and offer greater predictability regarding government use of a GPS tracking device. Rather than meet the new technology head-on, Justice Scalia reverted to notions of 19th Century tort law, using physical trespass as a lynchpin of the Fourth Amendment. Justice Scalia noted:

The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a “search” when it was adopted.49

Justice Scalia went on to cite Entick v. Carrington,50 to set up the importance of a property rights scheme to the law of search and seizure: “[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour’s close without his leave; if he does he is a trespasser, though he does no damage at all....”51

The Court proceeded to say that the text of the Fourth Amendment “reflects its close connection to property”52 and that therefore, “Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass at least until the latter half of the 20th Century.”53

The Court then placed Katz within this property-bound conception, stating that it is part of later cases that “deviated from that exclusively property-based approach.”54 Instead of recognizing Katz as replacing the property-bound understanding of prior generations, the Court instead declined to recognize the “reasonable expectation of privacy” standard as the sole yardstick, observing:

48 ___ U.S. at ___ (2012).
49 Id. at ___.
50 “Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765), is a case we have described as a ‘monument of English freedom’ ‘undoubtedly familiar’ to ‘every American statesman at the time the Constitution was adopted, and considered to be ‘the true and ultimate expression of constitutional law’ with regard to search and seizure.” Brower v. County of Inyo, 489 U.S. 593, 596 (1989)(quoting Boyd v. United States, 116 U.S. 616, 626 (1886)).

51 Jones, 565 U.S. at 4 (2012), citing Entick at 817.
52 Jones, 565 U.S. at N. 2 (2012) (Justice Scalia also noted in the footnote, “If Jones was not the owner he had at least the property rights of a bailee. The Court of Appeals concluded that the vehicle’s registration did not affect his ability to make a Fourth Amendment objection, ibid, and the Government has not challenged that determination here. We therefore do not consider the Fourth Amendment significance of Jones’s status.” Id.)
54 Id. at 5.
But we need not address the Government’s contentions, because Jones’s Fourth Amendment rights do not rise or fall with the Katz formulation. At bottom, we must “assur[e] preservation of that degree of privacy against government that existed when the Fourth amendment was adopted.”55

Instead of taking the invitation to revitalize the balancing test between privacy interests and police practices, the Court in Jones proffered a narrow ruling that still fit comfortably inside the pre-Katz spatial envelope.56 This reversion to a physical trespass regime was as much a comment on the mosaic spun by Katz as it was on the vitality of the trespass world.57

Justice Sotomayor’s and Justice Alito’s concurrence spun a different picture, with what is now called the “mosaic” theory. Under this approach, the collection of raw data can involve so much information that it becomes a bigger and better picture of private information than if left to its de-aggregated pieces. Justice Sotomayor noted where the justices had similar approaches: As JUSTICE ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the Katz test by shaping the evolution of societal privacy expectations. Post, at 10–11. Under that rubric, I agree with JUSTICE ALITO that, at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’ Post, at 13.”58

Justice Sotomayor opined that even short-term monitoring by the government could yield a Fourth Amendment search:

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to

55 Id. at 5. Citing Kyllo at 34, in essentially finding that Katz’s “reasonable expectation of privacy” test was not the exclusive standard for determining whether Fourth Amendment rights were violated.

56 The Supreme Court is not the only one that utilizes the physical world within which to create analogues to cyberspace. In The Cartoon Network v. CSC Holdings, Inc., 536 F.3d 121, 132 (2008); for example, the Court compared digital storage devices such as a DVR to an individual who owns a photocopy shop.

57 Instead of broadening the reach of the case to encompass the subtle and obvious shifts caused by a movement to a mobile, information-based, 24/7 decentralized communication-oriented society (where everyone could become a micro-broadcaster, photographer on the spot or leader of thousands of Twitter followers), it decided to stick with a decades-old framework. Instead of following a path it set-up in Arizona v. Gant, it went back much further to the notions of trespass in Olmstead.

58 Sotomayor, J., concurring opinion, United States v. Jones, 565 U.S. at __. 
assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may “alter the relationship between citizen and government in a way that is inimical to democratic society.” United States v. Cuevas-Perez, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention.

**C. The Search Incident to Lawful Arrest Exception**

A search incident to a lawful arrest is considered an exception to the warrant preference of the Fourth Amendment. According to Justice Scalia, “In *Chimel v. California*, 395 U.S. 752, 762—763 (1969), we held that a search incident to arrest was justified only as a means to find weapons the arrestee might use or evidence he might conceal or destroy. We accordingly limited such searches to the area within the suspect’s ‘immediate control’ – i.e., the area into which an arrestee might reach in order to grab a weapon or evidentiary item.”

The “immediate control” described in *Chimel* included a person’s “wingspan” and items within reach to which the arrestee had access. The Court set forth the narrower dual rationales for the exception, despite precedent for a broader basis for the rule.

The origins of the search incident to lawful arrest exception reach far into the past, into the English antecedents of American law. Judge Benjamin Cardozo, while on the N.Y. Court of Appeals, before his tenure on the United States Supreme Court, wrote in the case of *People v. Chigles*,

[T]here is one exception that has been established as firmly as the rule itself. The government may “search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime.” *Weeks v. United States*... There is no dearth of illustrative precedents both in our own country and abroad. *Dillon v. O’Brien*, 16 Cox C.C. 245; United States v. Snyder (D.C. 278 Fed. 650 ...).

59 *Id.*
Judge Cardozo hinted at a broader rationale than what has been considered the exception’s basis:

The right goes back beyond doubt to the days of the hue and cry, when there was short shrift for the thief who was caught “with the mainour,” still “in seisin of his crime.” 2 Pollock & Maitland History of English Law, 577, 578... The books speak broadly of searching the person of the prisoner for anything “that may be of use as evidence upon the trial.” (Thatcher v. Weeks, 79 Me. 547, 549, 11 Atl. 599), or for anything “that will aid in securing the conviction” (Holker v. Hennessey, 141 Mo. 527, 539, 42 S.W. 1090, 39 L.R.A. 165, 64 Am. St. Rep. 524; cf. Weeks v. United States, supra).

Justice Scalia, in his concurrence in Thornton v. United States, another case evaluating the scope of the exception, cited authorities for both a broad exception, allowing the search without any particularized justification and a narrower one, based on the dual rationales used today. Both approaches were viewed as deeply-rooted. The narrower approach, for example, had supporting authority dating back

---

64 Justice Scalia stated: “Numerous earlier authorities support this approach, referring to the general interest in gathering evidence related to the crime of arrest with no mention of the more specific interest in preventing its concealment or destruction. See United States v. Wilson, 163 F. 338, 340, 343 (CC SDNY 1908); Smith v. Jerome, 47 Misc. 22, 23—24, 93 N. Y. S. 202, 202—203 (1905); Thornton v. State, 117 Wis. 338, 346—347, 93 N. W. 1107, 1110 (1903); Ex parte Hurn, 92 Ala. 102, 112, 9 So. 515, 519—520 (1891); Thatcher v. Weeks, 79 Me. 547, 548—549, 11 A. 599, 599—600 (1887); 1 F. Wharton, Criminal Procedure §97, pp. 136—137 (J. Kerr 10th ed. 1918); 1 J. Bishop, Criminal Procedure §211, p. 127 (2d ed. 1872); cf. Spalding v. Preston, 21 Vt. 9, 15 (1848) (seizure authority); Queen v. Frost, 9 Car. & P. 129, 131—134 (1839) (same); King v. Kinsey, 7 Car. & P. 447 (1836) (same); King v. O'Donnell, 7 Car. & P. 138 (1835) (same); King v. Barnett, 3 Car. & P. 600, 601 (1829) (same).” Id. 541 U.S. at 629.
65 “Nevertheless, Chimel’s narrower focus on concealment or destruction of evidence also has historical support. See Holker v. Hennessey, 141 Mo. 527, 539—540, 42 S. W. 1090, 1093 (1897); Dillon v. O’Brien, 16 Cox C. C. 245, 250 (Ex. Div. Ire. 1887); Reifsnyder v. Lee, 44 Iowa 101, 103 (1876); S. Welch, Essay on the Office of Constable 17 (1758). And some of the authorities supporting the broader rule address only searches of the arrestee’s person, as to which Chimel’s limitation might fairly be implicit. Moreover, carried to its logical end, the broader rule is hard to reconcile with the influential case of Entick v. Carrington, 19 How. St. Tr. 1029, 1031, 1063—1074 (C. P. 1765) (disapproving search of plaintiff’s private papers under general warrant, despite arrest). But cf. Dillon, supra, at 250—251 (distinguishing Entick); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 303—304 (1967).” Id. at 630.
Interestingly, Justice Scalia believed both approaches met the reasonableness requirement of the Fourth Amendment: “In short, both Rabinowitz and Chimel are plausible accounts of what the Constitution requires, and neither is so persuasive as to justify departing from settled law.” Yet, in Thornton v. United States, Justice Scalia opted for the narrower approach because of the doctrine of stare decisis, adding this caveat:

But if we are going to continue to allow Belton searches on stare decisis grounds, we should at least be honest about why we are doing so. Belton cannot reasonably be explained as a mere application of Chimel. Rather, it is a return to the broader sort of search incident to arrest that we allowed before Chimel – limited, of course, to searches of motor vehicles, a category of “effects” which give rise to a reduced expectation of privacy, see Wyoming v. Houghton, 526 U.S. 295, 303 (1999), and heightened law enforcement needs, see id., at 304; Rabinowitz, 339 U.S., at 73 (Frankfurter, J., dissenting).

D. Development of the Search Incident to Lawful Arrest Doctrine

Several significant cases serve to develop the exception doctrine, recognizing its nuance and complexity, especially with respect to advancing technology of the times, such as the automobile and forensic science.

In United States v. Robinson, the Court was confronted with the question of whether a crumpled cigarette pack could be seized and searched as part of the exception. The Court’s analysis led to the “container” rule. In Robinson, the police lawfully arrested the defendant for driving without a license and then searched his person after the arrest. They found a crumpled cigarette pack and removed the contents, which were small packages of heroin.

The Court recognized the dual rationales for the search incident to arrest. These rationales, protecting officer safety and preventing the imminent destruction of evidence, applied to containers found on the arrestee, including the pack at issue.

In applying these rationales, the Robinson Court chose to adopt a bright-line test instead of a case-by-case analysis relying on the exigencies of the situation. Thus, the police were given a green light to conduct searches incident to lawful arrest of

---

66 Id. (Scalia, J., Concurring). S. Welch, Essay on the Office of Constable 17 (1758).”
68 Id. 541 U.S. at 631.
69 Id.
71 See Id. at 233–34.
arrestees regardless of any suspicion or cause to believe their safety was in danger or evidence would be compromised if they did not search. 72

*United States v. Edwards*73 provided a different fact pattern, coinciding with advances in forensic sleuthing.74 The case involved paint chips that could have been stuck to the arrestee’s clothing.

Finally, *Belton* and *Gant* provide an exploration of another technological advance, although it has been around for many generations, the automobile. The automobile, or motor vehicle, has created several recurring search incident to lawful arrest themes in the arrest of a driver or occupants of an automobile. Belton was seen as a way to deal with this recurring theme, and was motivated by a desire to construct “a straightforward rule, easily applied, and predictably enforced.”75

### III. Divided Outcomes in the Lower Courts

The courts that have confronted the issue of whether a search of a cellular phone falls within the search incident to lawful arrest exception have reached widely divergent results. The two cases in which certiorari petitions have been filed before the Supreme Court, *United States v. Wurie*76 and *Riley v. California*,77 also have different outcomes, facts, and rationales. Even the relevant technology levels of the cell phones are different, reflecting the continuing, almost dizzying advancements on a regular basis.

1. *United States v. Wurie*78

In *Wurie*, the defendant was arrested for selling drugs and taken to the police station, where two cell phones and keys were found on him. On one cell phone, there was an external caller ID screen that flipped open. The phone was not a “smart phone,” meaning it did not have Internet connectivity and mini-computer capabilities.79 The police observed the phone repeatedly receive calls from what appeared to be on the external screen a caller labeled “my house.” The officers

72 Id. at 235.
74 This area of the law was brought into the popular culture by television shows such as “C.S.I.” (Crime Scene Investigation), which are still occurring in various iterations, such as “C.S.I. Miami.”
75 453 U.S., at 459.
76 2013 WL 2129119, __ F.3d __ (1st Cir. 2013).
77 2013 WL 475232 (Cal. App. 2013)
78 2013 WL 2129119, __ F.3d __ (1st Cir. 2013).
79 The limited nature of the cell phone under consideration perhaps could be important in a case to reach the Supreme Court, since these phones would not have the same level of connectivity, informational storage capacity, or technological capacity.
opened the phone and saw on the wallpaper a picture of a woman and a child. The officers pressed a button to access the phone’s call log to see who had just called. The officers typed the phone number into the white pages phone directory to yield an address for the telephone number, which happened to be near where the defendant had parked his car. Judge Stahl stated:

This case requires us to decide whether the police, after seizing a cell phone from an individual’s person as part of his lawful arrest, can search the phone’s data without a warrant. We conclude that such a search exceeds the boundaries of the Fourth Amendment search-incident-to-arrest exception. Because the government has not argued that the search here was justified by exigent circumstances or any other exception to the warrant requirement, we reverse the denial of defendant-appellant Brima Wurie’s motion to suppress, vacate his conviction, and remand his case to the district court.\(^\text{80}\)

After reviewing the Supreme Court’s incident to lawful arrest decisions, from *Chimel*,\(^\text{81}\) to *Edwards*,\(^\text{82}\) to *Chadwick*,\(^\text{83}\) to *Gant*,\(^\text{84}\) the Court emphasized that a cell phone was far more than a mere container or wallet:

We suspect that the eighty-five percent of Americans who own cell phones and “use the devices to do much more than make phone calls,” Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, Pew Internet & American Life Project, 2 (Nov. 25, 2012), http://pewinternet.org/~/media/Reports/2012/PIP_CellActivities_11.25.pdf, would have some difficulty with the government’s view that “Wurie’s cell phone was indistinguishable from other kinds of personal possessions, like a cigarette package, wallet, pager, or address book, that fall within the search incident to arrest exception to the Fourth Amendment’s warrant requirement.” In reality, “a modern cell phone is a computer,” and “a computer ... is not just another purse or address book.” *Flores-Lopez*, 670 F.3d at 805. The storage capacity of today’s cell phones is immense. Apple’s iPhone 5 comes with up to sixty-four gigabytes of storage, see Apple, iPhone, Tech Specs, http://www.apple.com/iphone/specs.html (last visited May 16, 2013), which is enough to hold about “four million pages of Microsoft Word documents.”\(^\text{85}\)

\(^{80}\) *Wurie* at _____.  
\(^{82}\) 415 U.S. 800 (1974).  
\(^{84}\) 556 U.S. 332 (2009).  
\(^{85}\) *Id.* at _____. 
The Court focused on the nature of the search to distinguish a cell phone from other items seized in a search incident to a lawful arrest. The Court utilized the origins of the Fourth Amendment to advance the specter of discretionary police dragnets within a person's cell phone:

Just as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government's proposed rule would give law enforcement automatic access to “a virtual warehouse” of an individual's “most intimate communications and photographs without probable cause” if the individual is subject to a custodial arrest, even for something as minor as a traffic violation. Matthew E. Orso, Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence, 50 Santa Clara L.Rev. 183, 211 (2010). We are reminded of James Otis's concerns about “plac[ing] the liberty of every man in the hands of every petty officer.” Michael, supra, at 908 (citation and internal quotation marks omitted).

The Court conceded that the Supreme Court has not distinguished between the types of items found in such searches as a litmus test for legitimacy, but said the search of cellular phone devices are qualitatively different:

It is true that Robinson speaks broadly, and that the Supreme Court has never found the constitutionality of a search of the person incident to arrest to turn on the kind of item seized or its capacity to store private information. In our view, however, what distinguishes a warrantless search of the data within a modern cell phone from the inspection of an arrestee's cigarette pack or the examination of his clothing is not just the nature of the item searched, but the nature and scope of the search itself.

2. Riley v. California

In Riley, several men standing near Riley's car shot at the car of a rival gang member. Riley was implicated as one of the shooters. Later that month, the police stopped Riley while he was driving and decided to impound his car upon finding he was driving with an expired license. The police then conducted an impound inventory

86 Id. at
87 2013 WL 475232 (Cal. App. 2013)
search of the car and found several loaded handguns\textsuperscript{88} and “several indicia of gang affiliation.”\textsuperscript{89} Riley was arrested and his car impounded.

The Court focused on where the cell phone was found, noting:

> The key question is whether Riley’s cell phone was “immediately associated” with his “person” when he was stopped. (Diaz, supra, 51 Cal.4th at p. 93.) Relying on the evidence introduced at the suppression hearing, the trial court found the cell phone, which as I understand it was on [Riley’s] person at the time of the arrest, would fall into the category of a booking search, the scope of which is very broad,” and on this basis upheld the search. This finding, supported by the evidence, establishes that Riley’s cell phone was immediately associated with his person when he was arrested, and therefore the search of the cell phone was lawful whether or not an exigency still existed. (Diaz, supra, 51 Cal.4th at p. 93.)

3. Other Case Law: Deepening the Divide

There are other courts that have weighed in on the issue. Some of these courts, notably the Northern District of California,\textsuperscript{90} the Florida Supreme Court\textsuperscript{91} and the Ohio Supreme Court,\textsuperscript{92} have held that the search of a cell phone is not automatically permitted under the incident to lawful arrest exception when the phone is on or near an arrestee. These courts all found that the searches were not justified within the parameters of the traditional “walls and doors” authority.

In \textit{United States v. Park}, the Court in the Northern District of California found that the cell phone should be considered akin to a footlocker as in \textit{Chadwick v. State}.\textsuperscript{93} The Court consequently found that the reasoning behind the exception to searches incident to a lawful arrest was not met:

> The searches at issue here go far beyond the original rationales for searches incident to arrest, which were to remove weapons to ensure the safety of officers and bystanders, and the need to prevent concealment or destruction of evidence....Officers did not search the phones out of a concern for officer safety, or to prevent the concealment or destruction of evidence. Instead, the purpose was purely investigatory. Once the

\textsuperscript{88} As a result of subsequent ballistics testing, the bullets from the handguns matched the bullet casings found at the scene of the shooting earlier in the month. \textit{Id.} at 3.

\textsuperscript{89} \textit{Id.} at 8.

\textsuperscript{90} \textit{United States v. Park}, 2007 WL1521573 (N.D. Ca. 2007).

\textsuperscript{91} \textit{Smallwood v. State}, 2013 WL 1830961, _So.3d_ (2013).


\textsuperscript{93} 433 U.S. 1 (1977).
officers lawfully seized defendants’ cellular phones, officers could have sought a warrant to search the contents of the cellular phones.\textsuperscript{94}

In the Florida Supreme Court decision, \textit{Smallwood v. State},\textsuperscript{95} the Court viewed the search of a cell phone as the equivalent to accessing a person’s home:

In our view, allowing law enforcement to search an arrestee’s cell phone without a warrant is akin to providing law enforcement with a key to access the home of the arrestee. Physically entering the arrestee’s home office without a search warrant to look in his file cabinets or desk, or remotely accessing his bank accounts and medical records without a search warrant to look in his file cabinets or desk, or remotely accessing his bank accounts and medical records without a search warrant through an electronic cell phone, is essentially the same for many people in today's technologically advanced society. We refuse to authorize government intrusion into the most private and personal details of an arrestee’s life without a search warrant simply because the cellular phone device which stores that information is small enough to be carried on one’s person.\textsuperscript{96}

In \textit{State v. Smith},\textsuperscript{97} the Ohio Supreme Court found that a cell phone search did not trigger either of the dual rationales for such an exception, and that the \textit{Robinson} container conceptualization did not apply. The Court stated:

Objects falling under the banner of “closed container” have traditionally been physical objects capable of holding other physical objects. Indeed, the United States Supreme Court has stated that in this situation, “container” means any object capable of holding another object. \textit{New York v. Belton}.\textsuperscript{98}

A number of other lower courts have permitted the searches of cell phones incident to a lawful arrest without any additional justification. In addition to \textit{Riley v. California},\textsuperscript{99} these courts include the Fourth Circuit Court of Appeals in \textit{United States v. Murphy},\textsuperscript{100} the Fifth Circuit Court of Appeals in \textit{United States v. Finley},\textsuperscript{101} the Seventh Circuit Court of Appeals in \textit{United States v. Florez-Lopez},\textsuperscript{102} the Northern District of California in \textit{United States v. Park},\textsuperscript{103} the Supreme Court of California in

\begin{itemize}
  \item \textit{Smallwood v. State}, 2013 WL 475232.
  \item \textit{Id.} at 13.
  \item \textit{State v. Smith}, 920 N.E. 2d 949 (Ohio 2009).
  \item 920 N.E.2d at 954.
  \item \textit{See Riley}, supra, at N. ____.
  \item \textit{United States v. Murphy}, 552 F.3d 250 (4th Cir. 2009).
  \item \textit{United States v. Finley}, 477 F.3D 250 (5th CIR. 2007).
  \item \textit{United States v. Florez-Lopez}, 670 F.3d 803 (7th Cir. 2012).
  \item \textit{United States v. Park}, 2007 WL 1521573 (N.D. Cal. 2007).
\end{itemize}
People v. Diaz, the Supreme Judicial Court of Massachusetts in Commonwealth v. Phifer, and the Supreme Court of Georgia in Hawkins v State.

While the lower courts reached the same conclusion, that searches of cell phones incident to a lawful arrest are permissible within the established exception to the Fourth Amendment warrant preference, the rationales of these courts differed.

In Finley, the Court found that a cell phone was a type of container on the arrestee's person akin to the cigarette pack in Robinson, and was consequently fully subject to a search incident to a lawful arrest. The Court observed that it was well-settled that such a search is within the exception, but also qualifies as a reasonable search under the Fourth Amendment. The Court observed:

> Police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial. The permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person.

The Court in Park found that a cell phone was a possession within an arrestee's immediate control, essentially likening it to the footlocker in Chadwick, stating that “modern cellular phones have the capacity for storing immense amounts of private information.”

In United States v. Flores-Lopez, the Seventh Circuit Court of Appeals said the nature of the intrusion “might be so trivial that its seizure would not infringe the Fourth Amendment” at all, and used predigital parallels to justify a search of a cell phone incident to lawful arrest. The Court also noted, “We are quite a distance from the use of the iCam to view what is happening in the bedroom of the owner of the seized cell phone.” Finally, the Court recognized alternatives to searching the cell phone, including placing the phone in a Faraday bag or cage, which is “essentially an aluminum-foil wrap...which isolates the cell phone from the phone network and

---

104 People v. Diaz, 51 Cal. 4th 84 (Cal. 2011)
106 Hawkins v. State, 723 S.E.2d 924 (Ga. 2012)
107 Finley, 477 F.3d at 259-60.
109 Id. at 8.
110 670 F.3d at 807.
111 “It’s not even clear that we need a rule of law specific to cell phones or other computers. If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number. If allowed to leaf through a pocket address book, as they are, United States v Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993), they should be entitled to read the address book in a cell phone.” Id. at 807.
from Bluetooth and wireless Internet signals,” and to mirror or copy the cell phone’s contents “to preserve them should the phone be remotely wiped.”\textsuperscript{112}

Some courts prohibited searches after focusing on other aspects of phone searches than the invasion of privacy. In 2012 the Seventh Circuit Court of Appeals in \textit{United States v. Burgard}\textsuperscript{113} permitted a cellular phone to be seized but not searched as an incident to lawful arrest. In \textit{Burgard}, the Seventh Circuit Court of Appeals treated the delayed application for a warrant as unreasonable and a violation of the owner’s possessory rights,\textsuperscript{114} not privacy.\textsuperscript{115} This case aptly illustrates the intersection and overlap between property and privacy rights.

\section{Advancing Technology – Blurring the Bright Lines of Grand Theory}

\subsection{The New Realities Principle}

\begin{itemize}
  \item \textsuperscript{112} Id. at 807. The Court also cited the Department of Justice, Computer Crime and Intellectual Property Section, “Awareness Brief: Find My iPhone (June 18, 2009).
  \item \textsuperscript{113} 2012 WL 1071706, _F.3d_ (2012).
  \item \textsuperscript{114} The Seventh Circuit Court stated that the seizure “relates to any possessory interest in the seized object, not to privacy. . . . ‘A seizure affects only the person’s possessory interests; a search affects a person’s privacy interests.’ Segura v. U.S., \textit{supra}. The longer the police take to seek a warrant, the greater the infringement on the person’s possessory interest will be. . . . But unnecessary delays also undermine the criminal justice process in a more general way: they prevent the judiciary from promptly evaluating and correcting improper seizures.” \textit{Id. Burgard} at ___.
  \item \textsuperscript{115} When the government agents held the phone too long without obtaining a warrant, the case transformed into an analogue of \textit{United States v. Place}, intruding on the property right of possession. The Court stated:

  \begin{quote}
    [t]here is unfortunately no bright line past which a delay becomes unreasonable. Instead, the Supreme Court has dictated that courts must assess the reasonableness of a seizure by weighing ‘the nature and quality of the intrusion on the individual’s 4th Amendment interests against the importance of the governmental interests alleged to justify the intrusion.’ (citing \textit{U.S. v. Place}). \textit{Id. United States v. Burgard}.
  \end{quote}
\end{itemize}
Information is power” -- Kevin Mawae

From information aggregation to facial recognition software, different technological advances are seemingly made every day. Many advances involve private industry, but an equal number seem to involve government development or use.

Advances in technology enhance human perception, but do much more than that by changing facts, the pace and nature of daily life, and cultural understandings. We have become a “heads-down” society, for example, where people often socialize sitting near each other, occupied with their own cell phones or tablet devices. This not-looking-up socializing and 24/7 interconnectivity are becoming the dominant experience, rather than the exception. One new study suggests that “online and mobile technology have fundamentally changed the way Americans live and work over the past 15 years.”


117 Unmanned aerial drones have now been approved for commercial domestic surveillance uses. See Kadhim Shubber, First Domestic Surveillance Drones Approved for Commercial Surveillance in the US, Wired.co.uk, Technology (July 30, 2013). The article can be found at: http://www.wired.co.uk/news/archive/2013-07/30/FAA-approves-domestic-drones.

118 E.g., David Ingram, How Drones Are Used for Domestic Surveillance. The Christian Science Monitor (Reuters June 19, 2013). In the article, FBI Director Robert Mueller indicated that the unmanned aerial drone surveillance was only used to track stationary objects and to protect law enforcement personnel from serious risk of harm. The article can be found at: http://www.csmonitor.com/USA/Latest-News-Wires/2013/0619/How-drones-are-used-for-domestic-surveillance.

119 See, e.g., Larry Copeland, “Driven By Social Media, Millennials Do Less Driving,” USA Today, A4 (Oct. 2, 2013). “The first [report released at the American Public Transportation Association meeting] from the U.S. Public Interest Research Group, found that online and mobile technology have fundamentally changed the way Americans live and work over the past 15 years.” Id.

120 It was recently reported that a person openly brandishing a gun on a commuter train was not observed by many of the commuters because they were busy with their electronic devices. Laila Kearney, “Absorbed Smartphone Users Oblivious to Gunman Before Fatal Calif. Train Shooting,” NBC News (Oct. 10, 2013) (“When a California college student was killed by a gun-wielding stranger on a crowded commuter train in San Francisco, none of the dozens of passengers on board saw it coming; officials say they were too absorbed in their mobile devices.” Id.) The article can be found at: http://usnews.nbcnews.com/_news/2013/10/10/20895629-absorbed-smartphone-users-oblivious-to-gunman-before-fatal-calif-train-shooting?lite.

All told, the devices at the heart of these advances, such as tablets and cellular phones, are not merely accessories in the transition, but rather the instruments of new technology-based realities. These realities not only affect the experience of daily life but feature an increasing separation of form and function, where a phone is not just a phone – if it is primarily used that way at all – and a watch is not just a watch, and so on. The transformation of facts impacts legal rules and principles. Instead of a unified science upon which bright-line legal rules can rest, the legal rules have been forced to adapt through pluralized, localized frameworks. The best illustration is the significance of the automobile to the 20th Century legal analysis. The automobile, a major 20th Century tool for human transport, also served to transport contraband, to initiate contact between the public and the police, and as the locus for many arrests.

In addition to changing existing cultures, advancing technology has created new cultural realities. Technology has spawned an Internet culture, hacker culture, gamer culture and email cultures, all of which have gone through several iterations in their first decades of existence.

A. Themes of Advancing Technology

The technology advancements changing the face of society are often accompanied by several recurring themes. These themes include interconnectivity, mobility, elasticity, perpetual aggregation, and pluralism. While Ghandi once commented that

---

122 For example, social media has impacted how people travel. Young Americans, whose embrace of new technologies and social networking tools enable them to adopt new ways of getting around, are beginning to change the nation’s transportation landscape.” Larry Copeland, Id.

123 See, Larry Copeland, Id. “[Millenials] consider public transportation the best option for digital socializing and one of the most likely ways to connect with the communities they live in.”

124 These factual changes ought to be embraced in the law, particularly the pluralism forced by the regular technology advances. This pluralism creates local structures based on the actual facts, not universalist structures based on a one-size-fits-all.

125 It is much more difficult to define and maintain freedom from government and private intrusion given government-private partnerships and the routing of almost all information through third parties. An all-or-nothing definition of privacy no longer is functional. Information travels, is stored with various companies, and is accessible by many. Information has great value, from biometrics, to DNA, to social security and credit card numbers.

126 The newer generations are even described as being “born digital,” generations that have been aware of digital advancements virtually their entire lives. For this generation, for example, “The computer has always been king” Tom McBride and Ron Nief, The Mindset Lists of American History at 219 (John Wiley and Sons 2011), and “With caller ID they’ve always known who’s waiting on the line.” Id. at 208.
“life was not meant to be speeded up,” ever-increasing speed is a significant attribute of these advancements as well.127 The themes are transformational, often separating the form and function of objects from the predigital world. More specifically, they also change the way police investigate real and potential crime, altering deterrents, incentives, and efficiencies.

Interconnectivity is a significant theme of advancing technology, particularly over the past two decades. People are technologically interfaced and essentially interconnected during all waking hours – and even when they sleep. There is virtually no geographical isolation -- except for cell phone “dead” spots -- with big satellite dishes serving as symbolic and actual connectors even in remote places. Even the interfaces are growing, with biometric, health, purchasing and location data all subject to aggregation and sharing. Disclosure of information is required in many contexts, from purchasing on EBay or Amazon on the Internet, to getting email or bank information. The connectivity boundaries readily transcend countries to create a “world is flat” globalization.128

Developing technologies have created new forms of bundling of information that in the past would have been practically impossible to duplicate by human effort.129 A person can blast information worldwide almost instantaneously, with the power to change reputations, elections and even governments. Significantly, there is no ready recall130 for information once transmitted and that information often can be collected long after transmission, hanging for months or years – or even forever -- in

127 “Life was not meant to be speeded up.” –M. Ghandi
128 People are technologically interfaced and essentially interconnected during all waking hours. There is virtually no isolation, with big satellite dishes serving as symbolic and actual connectors even in remote places. Disclosure of information is required in many limited contexts, from purchasing on EBay or Amazon on the Internet, to getting email or bank information. Who wants to know? The answer is many interested parties, from the State, to advertisers who track people’s actions on the Internet, to companies, to friends and curious on-lookers all have an interest in information, which has grown into a currency likely completely unforeseen only decades before. The informational types are multiplying. DNA, genetic info, biometrics (iris, fingerprints, hair properties).
129 For example, advancing surveillance technologies, such as Global Positioning Systems (GPS), have allowed much easier access to information and created greater accuracy.
130 As a billboard alongside a road in NC aptly exclaimed, “Words are powerful, be careful how you use them.”
the Internet ether.\textsuperscript{131} Often, this information is invisible to most of us, serving as part of a wired and wireless technocracy infrastructure.\textsuperscript{132}

The mobility of cellular phones is almost taken for granted, particularly when compared to the land telephone lines that many houses no longer use. Even the first mobile phones now look awkward, big and antiquated.

The elasticity of information and technological development is another significant feature. How information is aggregated and where can change its nature. These aggregations are often invisible to the human eye.\textsuperscript{133} Whether the information is for a shopping or police data base, for example, will determine how it is grouped.

The scope of the data created by technology cannot be underestimated. The huge quantities that can be stored and accessed from data based provide new opportunities and sedimentary layers for historical sleuthing.\textsuperscript{134} A person can blast information worldwide almost instantaneously, with the power to change reputations, elections and even governments. The data created can exist in perpetuity, creating a trail for others, years and decades later, to follow and refresh.

\textbf{B. 20\textsuperscript{th} Century – Automobiles}

When one looks for advancing technology that transforms Fourth Amendment analysis, one need look no further than the automobile, which also transformed much of society during its development. The innovations with the automobile directly involved connectivity and more mobile rapid transit for the masses. The innovations extended to mass production techniques,\textsuperscript{135} as well as efficiencies, and

\textsuperscript{131} From recalled emails, to Twitter blasts, to YouTube posts to stored emails long forgotten, the fossilized imprint often remains to be seen not just by the archeological finder, but by millions who have access to a computer.

\textsuperscript{132} Some sites aggregate information disclosed in different places, yielding a whole that is greater and more dangerous than its parts. Others create information of value, such as biometrics.

\textsuperscript{133} In fact, the F.B.I. Director, Robert Mueller, recently conceded that drones indeed have been used for some “very minimal” domestic surveillance operations. Phil Mattingly, \textit{FBI Uses Drones in Domestic Surveillance}, Bloomberg News (June 19, 2013)(The Director made his comments in Senate testimony.) The article can be found at: http://www.bloomberg.com/news/2013-06-19/fbi-uses-drones-in-domestic-surveillance-mueller-says.html

\textsuperscript{134} The data is equivalent to sedimentary layers of rock, although developing at lightning speed in a more visible fashion.

\textsuperscript{135} “Committed to large-volume production of the Model T, Ford innovated modern mass production techniques at his new Highland Park, Michigan, plant, which opened in 1910 (although he did not introduce the moving assembly line until 1913-1914)... The basic differences that distinguish post-World War II models from the
styling, so that it became a staple for the 20th Century family. Particularly in the area of criminal procedure and Fourth Amendment analysis, the automobile has played a large role in 20th Century development of the doctrine. Since so many initial contacts and subsequent arrests occur between police and citizens in and relating to automobiles, search and seizures incident to arrest doctrine was forced to create structures dealing specifically with what was permissible and what was not within this context.

From *Carroll v. United States*, decided in 1925, was one of the first cases to note the distinction between a search of a house and a search of an automobile for contraband. The Court observed that the Fourth Amendment prohibits only unreasonable searches, and that a search of a car, if probable cause exists, could be reasonable, even without a warrant.

The special development of case law in the Supreme Court occurred with searches incident to arrest as well, starting with *Belton* and leading to *Gant*.

**C. 21st Century Devices- Computers, Phones, Stingrays, Data Accumulators**

“The world isn’t run by weapons anymore, or energy, or money. It’s run by little ones and zeroes, little bits of data. It’s all just electrons.”

Model T were in place by the late 1920s—the self-starter, the closed all-steel body, the high-compression engine, hydraulic brakes, syncromesh transmission, and low-pressure balloon tires. The remaining innovations—the automatic transmission and drop-frame construction—came in the 1930s.” Automobiles, [http://www.history.com/topics/automobiles](http://www.history.com/topics/automobiles) (Oct. 2, 2013).

To meet the challenges of market saturation and technological stagnation, General Motors under the leadership of Alfred P. Sloan, Jr., in the 1920s and 1930s innovated planned obsolescence of product and put a new emphasis on styling, exemplified in the largely cosmetic annual model change—a planned triennial major restyling to coincide with the economics of die life and with annual minor face-liftings in between.” Automobiles, [http://www.history.com/topics/automobiles](http://www.history.com/topics/automobiles) (Oct. 2, 2013).

While the automobile was developed in both Europe and the United States in the late 1800s, the vehicle was developed for the masses by the Ford Motor Company and others in the United States.

*471 U.S. 386 (1985).*

*Carroll v. United States, 267 U.S. 132 (1925)*

*Sneakers* (Universal Pictures 1992)
1. Technological Advances Generally

Innovative twenty-first century technology devices are developed for the general population and targeted for specific groups or individuals. New police techniques using these devices change the parameters of the Fourth Amendment conversation, from “hypothetically” to “realistically.” These devices often revolve around computers and multi-function equipment. The capacity of computers has increased exponentially since their development in the last part of the 20th Century. These super-computers are now being run in cellular telephones, creating the “smart” phone.

The development of digital-world devices has produced corollary developments in research and development for groups and individuals interested in accessing the newer devices. These groups, such as government entities, corporations, and the hacking world, want to gain access to devices through digital walls and doors. For example, there have been reports that the National Security Agency has the keys to most of the encryption used to protect Internet transmissions, and "backdoors created in many of the devices, such as in telephone switches, permitting the government to more easily tap phones and calls through Digital Collection System Network technology. In addition, computer spyware has been developed creating an invisible backdoor to computers that can monitor computer keystrokes remotely, from a distance. Even if a computer is disconnected from the Internet, the monitor is still subject to remote viewing through technology called Van Eck Phreaking. Because all electronics give off radio waves, tools can detect these waves remotely and determine what is on the computer screen.

141 Eyder Peralta, “Reports: NSA Has Keys of Most Internet Encryption,” NPR, September 5, 2013. The author noted:

The National Security Agency has the keys to most Internet encryption methods and it has gotten them by using supercomputers to break them and by enlisting the help of private IT companies, The New York Times and The Guardian are reporting.

In plain English, this means that many of the tools – like TLS, used by many banks and email providers – that people worldwide have come to believe protect them from snooping by criminals and governments are essentially worthless when it comes to the NSA. Id.

142 Dan Seitz, “6 New Spy Technologies You Literally Can’t Hide From,” (Sept. 20, 2010)

143 See generally, Viruses, Spyware and Malware, Information Services & Technology, M.I.T. The page was last viewed on August 30, 2013. It can be found at: http://ist.mit.edu/security/malware.

144 This technology gets its name from its discoverer, Wim van Eck.

145 Seitz, supra n. ____.
Devices are being used not only to augment sensory perception, but also to replace humans and animals in specific, functional ways. For example, there have been recent efforts to create the electronic equivalent of the dog sniff, thereby replacing the trained animal with a machine. While this would not necessarily change the Fourth Amendment analysis, it would again force an adjustment in the reality of crime interdiction.

2. Cell Phones – Multifunctional Pocket Computers

Cell phones, which apparently were introduced commercially by Motorola in the early 1970s, are now used worldwide. The number of users is growing exponentially. In June 2010, there were 292.8 million cell phone users in the United States alone. The number of mobile-only Internet users is anticipated to increase five times from what it is today and the amount of information processed on mobile, smart phone devices, is expected to increase forty-seven times from what it is today in the next five years. While it was initially and primarily used to make telephone calls, it has become a multifunctional tool that can more appropriately be called a pocket super-computer. The consequences for telephonic communications are astounding. A phone is not a phone anymore. What is a phone, after all, a container, transportation device, tracking device, portal, linkage device, or some combination of these and other analogues?

It was not long ago that supercomputers took up several large rooms and were measured in multiples of cubic feet. Over the years, as computing times rapidly increased and the space required shrank, it was only a matter of time before these computers were married to the cellular phone. So-called “smart” phones are much

---

146 See Lara Farrar, *Electronic Nose Could Spark End of Sniffer Dogs*, CNN.com (August 1, 2008). The National Science Foundation gave an engineering professor at the University of California, Riverside a grant of almost $1 million to pursue the project. *Id.* The article can be found at: http://www.cnn.com/2008/TECH/science/08/01/electro.nose/.


more than phones. These devices can contain large amounts of data, photos, financial records, emails, instant messages, and personal notes and information.\footnote{See, e.g., Jake Laperruque, “CDT Asks Supreme Court to Bar Warrantless Search of Cell Phones” Center for Democracy & Technology (Sept. 5, 2013)}

The cell phones store and utilize very personal information,\footnote{See, e.g., Orin Kerr, “Foreword: Accounting for Technological Change,” 36 Harv. J. of Law and Pub. Pol. 403 (2013) “Much of the information stored in a person’s cellular phone is deeply personal. The information can include photographs, text messages, e-mails, personal notes, records of visited websites, and many other kinds of personal information.”} from information relating to personal health, family, religion, and critical decisions relating to autonomy (e.g., abortion, illness, doctors and even personal hygiene). The apps contained on phones, combined with the photos stored in it, the notes taken, the emails and text messages, and the calendar, listing all professional and personal appointments, can create a quite detailed and private picture of a person. This picture might be more complete than even that know by friends and business colleagues.

Cell phone technology is expanding exponentially. In development are Near-Field Communication (NFC),\footnote{This technology permits cell phones to communicate directly with each other. The phones are held back-to-back and the phones can swap information, such as browser pages. A significant use is to allow one device to read another to make a commercial transaction. Companies such as McDonald’s and Walgreens have adopted some NFC-equipped terminals for use with this technology. John Brandon, “8 Groundbreaking Mobile Tech Advancements for 2012,” Popular Mechanics (1/28/13) www.popularmechanics.com/technology/gadgets/news/8-groundbreaking-mobile-tech-advancements-for-2012#slide-1 (last viewed, 1/27/13).} Bluetooth health device protocol, connecting a phone to heart monitors, the exercise bike and pedometer sensors, mobile security through CarrierIQ, smart skin phones,\footnote{Samsung is developing this technology, described as a “smart device-skin.” It has sought a patent for this technology.} that will take any digital image and display it across the skin of the phone, and a combination phone, laptop tablet and digital camera.\footnote{See, e.g., the Fujitsu Lifebook, scheduled for production in 2013.}

To protect the phone’s data, features included remote tracing or wiping of information. Newer phones have an activation lock that requires a password for reactivation, and a custom message displayed even after a remote erase.\footnote{The iOS7 software offers these features on the new iPhone 5s. See Wilson Rothman, “Activation Lock May Be Most Important iOS7 Feature,” Technology, NBC News (September 2013).}
feature is designed to deter theft of the phone for resale.\textsuperscript{158} The iPhone 5s features a fingerprint-scanning touch identification.\textsuperscript{159}

The computing functions of the phone create huge amounts of data. Significantly, so does the phone’s location. To promote the best cell phone tower signal, cellular telephones are tracked by cell phone companies. This tracking provides the phones with the best signal possible. The devices can now be tracked within feet of their location. This data, known as historical cell phone location information, provides a fairly accurate picture of the movements of the cell phone throughout a day – and its owner.

Cell phone tracking can occur with substitutes for the towers. Stingrays, also called International Monitor Surveillance Instruments (IMSI), are devices that mimic cell phone towers to collect location data on nearby cell phones.\textsuperscript{160} Data from all cell phones within a given range are received, including phones not targeted. Police departments in several states have used IMSI devices in crime interdiction.

2. “Smart” Watches

The separation of form and function can be even more clearly seen in the development of the “smart” watch.\textsuperscript{161} The watch tells time, but again is multi-

\textsuperscript{158} \textit{Id.} As several leading prosecutors have noted:

In the months ahead, it is our hope that Activation Lock will prove to be an effective deterrent to theft, and that the widespread use of this new system will end the victimization of iPhone users, as thieves learn that the devices have no value on the secondary market. We are particularly pleased that – because Activation Lock is a feature associated with Apple’s new operating system as opposed to a new device – it will be available to consumers with older phone models who download the free upgrade.” Joint Statement by San Francisco District Attorney, George Gascon and New York Attorney General Eric T. Schneiderman. \textit{Id.}

\textsuperscript{159} See, e.g., iPhone 5s, \texttt{www.apple.com}.

\textsuperscript{160} Stingrays track phones within a given range, and obtain information about phones not targeted. Government investigators, including the FBI, have been using stingrays since the 1990s. See Declan McCullagh, \textit{FBI Prepares to Defend ‘Stingray’ Cell Phone Tracking}, CNET News (March 27, 2013). The article can be found at: http://news.cnet.com/8301-13578_3-57576690-38/fbi-prepares-to-defend-stingray-cell-phone-tracking/.

\textsuperscript{161} The advertisement for a “Pebble” smart watch indicates its versatility: “Pebble is the first watch built for the 21st century. It’s infinitely customizable, with beautiful
functional. It contains computing functions and has the capability of making phone calls as well. While it might be worn as a watch, such an item is functionally less a watch than simply another form of interconnective device.

3. “Smart” Glasses (Google Glasses)

Just like there are now “smart” Internet-connectable devices, “smart” glasses have been developed as well. The Google company has created Google Glass, worn like a pair of eyeglasses, but calling it that would be a misnomer, given it is so much more of a multifunctional device than a monochromatic tool. Google Glass can record what the wearer sees, can send a message by telling it to do so, can share what is seen, and can produce directions on the glass.\textsuperscript{162}

C. 21\textsuperscript{st} Century Spying-Devices

Not only has advancing technology seen the creation of numerous devices, such as cellular telephones, GPS systems, and stingrays, but for every advance has been a countervailing effort to negate or parry the advance through the creation of a spying device. For example, Modern Data Extraction Devices (DEDs) can extract information from cellphones and other advances.\textsuperscript{163} The DEDs can obtain call history, email, contacts, calendars and even passwords.\textsuperscript{164} When Apple created an iPhone with fingerprint identification to deter thefts and promote security, the site istouchIDhackedyet.com was created. When the fingerprint system was allegedly hacked through the use of a fake duplicate print, it made national news.\textsuperscript{165}

IV. The Separation of Form and Function in a Post-Digital World -- Why Pre-Digital Analogues Will Not Work

Because the physical world parameters do not directly apply to advancing technology enhancements of sensory perception, courts have used many analogues downloadable watch faces and useful internet-connected apps. Pebble connects to iPhone and Android smart phones using Bluetooth, alerting you with a silent vibration to incoming calls, emails and messages. While designing Pebble, we strove to create a minimalist yet fashionable product that seamlessly blends into everyday life.” http://getpebble.com. The Web Site indicated there were “85,000 users and counting.” (last visit, October 2, 2013).


\textsuperscript{163} Electronic Privacy Information Center, Riley v. California, Top News.

\textsuperscript{164} Id. Other information that can be obtained includes location information, GPS fixes, media files, chats, and SMS messages.

to categorize the post-digital cases. These analogues draw many comparisons, leading to a variety of conclusions allegedly neutral, based on an objective comparison. What this section argues is that the analogues are based on local structures and reality-changing facts, often creating a poor fit for the comparisons.\textsuperscript{166}

The use of comparison is apparent in the realm of cellular telephone searches incident to a lawful arrest. What is the proper analogue in the physical world for cellular telephones, a digital device that seems to add features daily? It is clear that while they are still called “phones,” they are much more than that, and their functionality has grown in such a way that their telephonic capabilities play a diminishing role for some possessors. Instead, cellular telephones can be aptly described as two-way radios, as trackers, as data aggregators, as data and information storage containers, as lockable devices, as a transformational device for the 21\textsuperscript{st} Century in the way that the automobile was a transformational device for the 20\textsuperscript{th} Century, and as portals to information, past, present and future. The nature of the comparison makes a difference, particularly when trying to locate the devices within the Fourth Amendment framework in the case law of the pre-digital, physical world.

The analogues are explored in greater detail below.

1. \textit{Analogue #1: Physical Proximity}

The nexus or proximity approach provides the broadest and most abstract approach to analyzing cellular phone searches incident to a lawful arrest. It offers the functional equivalent of the trespass test championed by Justice Scalia in \textit{Jones v. United States} and is fully based on the pre-digital physical world, about space and physical distance. This approach has the advantage of creating bright lines. If the object is within the wingspan of the arrestee, it may be searched without justification, subject to exceptions, as exemplified by \textit{Arizona v. Gant}.

\textsuperscript{166} Even Justice Alito, in his concurrence in \textit{United States v. Jones}, notes that earlier analogues do not work when it comes to GPS technology: “The Court argues—and I agree—that 'we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” Ante, at 5 (quoting \textit{Kyllo v. United States}, 533 U. S. 27, 34 (2001)). But it is almost impossible to think of late- 18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach’s owner?” \textit{Id.} Justice Alito goes on to say, “The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.” \textit{Id.} at FN3.
This approach is characterized by *Olmstead v. United States* and *Jones v. United States*. In *Olmstead v. United States*, the Supreme Court found that the Fourth Amendment does not protect telephone wires from a home to the outside world. The Court found that the wiretapping was not a violation of the Fourth Amendment because there was no actual “entry of the houses or offices of the defendants.” *Olmstead* offered a property and tort law analysis of trespass in defining the scope of the Fourth Amendment. *Jones*, involving a GPS device placed on the defendant’s car without a valid warrant, was decided based on the physical trespass involved.

The problem with this approach is that it provides no limits to the search of the objects within an arrestee’s wingspan and does not provide any useful way of dealing with new multi-functional devices. In these ways, the proximity test overlooks the teachings of *Carney* and *Kyllo* by stopping the evolution of reality in the late 20th Century. Some illustrations help explain this critique. If a person is arrested while standing near a desk-top computer, would a full search of the contents of the computer, without any reasonable belief that the computer contains evidence, be lawful? If yes, would there be any limits on the search of photographs, email, and sites accessed by the user within the past year or years? Perhaps most significantly, if the machine’s data was stored on a cloud, could the police access the cloud as well as the device itself if the device contained the access information?

Now suppose a phone has remote capacities, meaning it could access cameras and other machines remotely. Would those be subject to access as well. For example, remote cameras can be placed in a home and remotely accessed on a cellular telephone. Would a search of the phone permit the application to be activated and the inside of the home viewed, without any more justification than the phone was found on a person during an arrest?

Further suppose that the device was password protected and the lock was activated. Would that make a difference in the search? How about if it was fingerprint protected, could the police force individuals to open their own phones for a search? What if a person was able to hit a button that erased the data on the phone so that a police officer found nothing. Could the police take the phone back to the lab to reconstruct the data on it?

The pre-digital Fourth Amendment cases further show how technology undermines the proximity test. In *California v. Ciraolo*, 476 U.S. 207 (1986), the Court described a boundary for searches by reaffirming the doctrine of “open fields,” which

-------------------

167 277 U.S. 438 (1928).
168 Id. at ___.
169 For example, the Belkin Company Netcam can be purchased for less than $150, plugged in to a ubiquitous electrical outlet, and operated through a downloaded application. It provides not only daytime surveillance, but is equipped with infrared technology to permit night views as well. Furthermore, it is equipped with a microphone to allow for real-time audio surveillance as well.
170 *Id.* at 213-214.
negated Fourth Amendment protection for areas that extended outside of a house into areas that might not be a field or even open. Significantly, the Court looked at the physically nonobtrusive manner in which the officers' observations took place, noting that the officers could see marijuana plants on the defendant’s private property with the naked eye. This doctrine essentially limited the right of privacy in private property exposed to the public. The Court also distinguished the part of the property surrounding a house called the curtilage.”

What if the cellular telephone had photos of the house and curtilage on it. Are those areas no longer private? Could the police use those photos to then get a warrant on a different issue than the arrest to enter the house and curtilage?

It becomes clear that “on-the-ground” functional equivalents to the days of physical surveillance and actual sensory perception are distorted and sometimes fully eclipsed by advancing technology.

---

171 "The observations by Officers Shutz and Rodriguez in this case took place within public navigable airspace"), see 49 U.S.C.App. § 1304, in a physically nonintrusive manner; from this point they were able to observe plants readily discernible to the naked eye as marijuana.”  Id. at 212.

172  Id. at 212:

“At common law, the curtilage is the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life.”  Oliver, supra, 466 U.S., at 180 (quoting Boyd v. United States, 116 U.S. 616, 630 (1866). See 4 Blackstone, Commentaries *225. The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened. The claimed area here was immediately adjacent to a suburban home, surrounded by high double fences.”  Id.

173 United States v. Knotts 460 U.S. 276, 278 (1983), offered the Supreme Court an initial foray into the government use of beepers to track private individuals in public. The Court found that the beeper, used on a codefendant of Knotts, a Mr. Petschen, was constitutional. The Court offered the analogue that the beeper was the functional equivalent of on-the-ground police surveillance. In other words, had the police been on the street, they could have seen the codefendant driving from the city to Knotts' remote cabin. “This fact, along with others, was used by the government in obtaining a search warrant, which led to the discovery of the clandestine drug laboratory. But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.”  Id at 282. The Court concluded that Knotts had an expectation of privacy in the interior of his cabin (which was not infringed). Id. at 285 (“But no such expectation of privacy extended to the visual observation of Petschen's automobile
2. Analogue #2: *Robinson*\textsuperscript{174} Containers

This analogue treats a cellular phone like the cigarette pack in *Robinson* – as a container fully within the automatic search zone of police when accomplished incident to a lawful arrest. To some extent, even “smart” phones are containers – containing hardware circuitry, as well as thousands of documents, photos and other bits of information. Fake phones, of course, can be hollowed out to serve as disguised containers of contraband and other material. Thus, the transition from the *Robinson* idea of a physical container that could contain contraband or a weapon to the idea of the phone as a data storage device appears to be consistent.

While cellular phones technically are containers, incorporating within their shells hardware circuitry and physical screws and such holding them together, these devices are not functional containers. That is, they generally are not used by the possessor to contain things, such as a backpack or wallet. While the rhetorical statement is that the device “contains” information – email, photos, etc. -- these are not in their physical forms, but in code, allowing the storage of thousands of documents, photos and videos. Further, while trickery and deception could be applied to disguise a container (or weapon) as a cellular phone, the objects’ overwhelming usage is as a multifunctional communications tool.

3. Analogue #3: *Chadwick*\textsuperscript{175} Footlockers

In *Chadwick* the court found:

> Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might arriving on his premises after leaving a public highway, nor to movements of objects such as the drum of chloroform outside the cabin in the “open fields.” *Hester v. United States*, 265 U.S. 57 (1924).”\textsuperscript{175} Of course, there is no exact analogue to post-digital surveillance here. Petschen, aware that he was manufacturing illegal drugs at the remote cabin, likely had a heightened sense of awareness regarding the possibility that he was being surveilled during his drive from the store to the cabin, as evidenced by his evasive maneuvering during the drive. *Id.* His evasive maneuvering was at least partially successful, causing the police to drop the live police tail. *Id.*

\textsuperscript{174} 433 U.S. 1 (1977).

\textsuperscript{175} 433 U.S. 1 (1977).
gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.\textsuperscript{176}

This conception can be applied to cellular phones, particularly those that are password protected, fingerprint protected or otherwise locked. Phones are like footlockers in that once securely within government possession, they are not likely to create an imminent danger of harm to the police or contain evidence in danger of imminent destruction.

This analogy only goes so far. The capabilities of a cellular telephone far outstrip a footlocker, and the kinds of activities and contents on a phone has a huge range, again qualitatively and quantitatively different than the storage device. Few people would confuse cellular telephones with luggage; and fewer still would use the two for the same purposes. Further, the cellular phone might indeed be a part of the crime for which the suspect was arrested, such as selling drugs with the phone. In \textit{People v. Diaz},\textsuperscript{177} for example, the defendant was arrested after driving a car allegedly shepherding buyers of drugs to the seller. The defendant vehemently denied any involvement. After the police viewed the suspect’s phone, they found an instant message stating, “6-4-80.” This message, they believed, was a code for a drug sale, “Six of the drug items for $80.” After the police confronted the defendant with this new information, the defendant confessed.

4. Analogue #4: \textit{Gant}\textsuperscript{178} Automobiles

Cellular phones are the modern day automobiles, some suggest, and should be treated similarly.\textsuperscript{179} The approach taken by the Supreme Court to automobiles

\begin{footnotesize}
\textsuperscript{176} 433 U.S. at 15.
\textsuperscript{177} \textit{People v. Diaz}, 51 Cal.4th 84 (2011).
\textsuperscript{178} 556 U.S. 332 (2009).
\textsuperscript{179} While some commentators might object to fact-specific rules under the Fourth amendment, Professor Orin Kerr offered a thoughtful rebuttal: How can we justify one rule for physical evidence and another rule for digital evidence? I have two answers. The first is that technology-specific rules can be appropriate when technologies create recurring facts. With- in Fourth Amendment law, the automobile provides the obvious example. A large chunk of Fourth Amendment doctrine concerns automobile-specific rules. Examples include the automobile exception to the warrant requirement, rules on when automobiles can be stopped, when passengers can be ordered out of the car, and when cars can be searched incident to a driver’s arrest..... Second, whether technology-specific rules appear natural or awkward depends on when along the technology timeline you look.” Orin S. Kerr, “Foreword: Accounting for Technological Change,” 36 Harv. J. of L. and Pub. Pol. 403, 407 (2013).
\end{footnotesize}
generally, requiring reasonable suspicion to stop and probable cause to search, and to searches incident to the arrest of persons in automobiles, provides a framework for use in the detention and search of cellular phones. Professor Orin Kerr provides a provocative and thoughtful comparison:

In my view, sensible guidance for new rules governing the search of digital storage devices incident to arrest is provided by existing doctrine on searching automobiles in those circumstances. Like cell phones, cars are mobile. And like cell phones, cars can store a great deal of personal information. As the Court recognized in Arizona v. Gant, allowing a complete search of a car as a routine matter whenever the driver has been arrested permits a search far beyond the rationales of the exception. Under Gant, officers can search the car only in two circumstances: first, “when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search,” and second, when “it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.”

Professor Kerr further suggested that automobile-specific rules fit existing Fourth Amendment doctrine, arguing that the Supreme Court has adjusted its doctrine to changing facts to moderate the balance of power between the government and individual. Autos were transformational because in addition to providing a new and upgraded form of transportation, autos also served as advantageous criminal transport tools, facilitating crime. This was especially true during prohibition, when cars were the primary transport devices used for illicit alcohol. Consequently, as a form of contraband, cars lost some of the privacy envelope that surrounded them.

Yet, cellular phones are not used to commit crimes in as central a manner as autos, although text messaging is indeed used sometimes as such. Rather, cellular phones are more accurately multi-functional tools, doing many more things than the automobile, which still is primarily used for transportation purposes. Further, the automobile is a more conventional storage container, with a trunk and glove box specifically designed for the storage of physical things. While the rationale of Gant can be readily transferred to cell phone searches incident to a lawful arrest, it does not mean that phones are just like autos and should be treated similarly.

5. Analogue #5: Houses

Cellular telephones can be equated with houses or homes in that phones are used to express and communicate with others on sensitive personal matters, often via text, email, photos or other forms of messaging, store this information for ready access,

---

182 Id., Kerr at 502.
183 Id. at ____. 
and paint an intimate picture of the phone’s owner if another was permitted to
rummage through it. The phone can show who the owner’s associates are, what is
on their calendar, what doctors they are seeing, what medications they are taking,
and what social media they are on and in what way.

Yet, for all of the similarities to a house, people do not sleep or otherwise live in
their phones and the phones are just as likely to be accessed on a crowded plane as
in a private location with a closed door. While the “head-down” society shows that
people in many ways are completely preoccupied with their phones, the phones are
not a home-substitute.

V. The Best Option -- Using Post-Digital Local Structures to Evaluate the
New Realities of Cell Phone Searches

“Law is a distinctive way of imagining the real.” Cifford Geertz

A. Defining Local Structures

Trying to fit localized and new facts into an earlier reality provides for a bad fit and
generally, bad results. The analogues above illustrate how the continued reliance on
outdated facts diminish and eviscerate the parallels. Yet, an alternative protocol
exists, that of local structures.

Local structures simply recognize the need for legal analyses to assess the facts
created and distorted by advancing technologies. Local structures are pluralistic,
focusing on frameworks within the applicable context. Local frameworks embrace
the new realities principle. Instead of attempting to utilize a unified legal theory
such as trespass or proximity, local structures use factors, such as police discretion
and intent, the nature, scope and aggregation of enhancement of physical
perception, and degree and nature of intrusiveness.

B. Applying Local Structures

To apply local structures in the search incident to lawful arrest context, focusing on
the various facts associated with the arrest will be important, down to what the
police accessed, to the type of cellular phone, to the intent and discretion exercised
by the police, to the nature and degree the police enhanced their physical perception
through accessing the cellular phone.

A judge’s description of the Belton184 bright line rule for auto searches incident to
lawful arrest mirrors the argument about cell phone searches: “[I]n our search for
clarity, we have now abandoned our constitutional moorings and floated to a place
where the law approves of purely exploratory searches of vehicles during which
officers with no definite objective or reason for the search are allowed to rummage

184
around in a car to see what they might find.”\textsuperscript{185} Carney\textsuperscript{186} and Kyllo\textsuperscript{187} provide a glimpse of how this issue can be aptly handled through the use of local structures.

1. Using Existing Precedent: Kyllo,\textsuperscript{188} Carney,\textsuperscript{189} and Cotterman\textsuperscript{190}

   a. Kyllo\textsuperscript{191}

Kyllo provides the Court’s first advancing technology case on the cusp of the digital world. While the court appeared ready to confront the reality-changing nature of the infra-red technology involved, it was not ready to provide an assessment of how much technology enhancement of perception would render police action a search:

   The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much. While we upheld enhanced aerial photography of an industrial complex in Dow Chemical, we noted that we found “it important that this is not an area immediately adjacent to a private home, where privacy expectations are most heightened.”\textsuperscript{192}

Instead, the Court had a familiar locus to wrap its opinion around – government invasiveness of a house:

   While it may be difficult to refine Katz when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences is at issue, in the case of the search of the interior of homes-the prototypical and hence most commonly litigated area of protected privacy-there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of

\begin{flushleft}
\textsuperscript{185} McLaughlin, supra, at 894 (Trott, J., concurring).
\textsuperscript{186} 471 U.S. 386 (1985).
\textsuperscript{187} 533 U.S. 27 (2001).
\textsuperscript{188} Id.
\textsuperscript{189} 471 U.S. 386 (1985).
\textsuperscript{190} Docket No. 09-10139 (March 8, 2013)(en banc)
\textsuperscript{191} 533 U.S. 27 (2001).
\textsuperscript{192} Id. at 33.
\end{flushleft}
the home that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area,” Silverman, 365 U.S., at 512, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.193

Yet, the Court did touch upon the noxiousness of enhancing senses to create a new door into the interior of a house—regardless of the lack of physical intrusion of the police.

b. California v. Carney194

California v. Carney shows how the Court handles multifunctionality. In Carney, the Court had to decide whether to treat a Road Vehicle (RV), “a fully mobile motor home,”195 as an automobile, home, or combination of the two for purposes of a search. The Court focused on its use as a vehicle in generally classifying it within the automobile category, with one notable exception. The Court considered the advance in technology as part of its analysis, which is exactly what it should do even when technology provides new cultural realities and facts.

Carney shows how courts can deal with cellular telephones. When carried as multifunctional computers, they ought to be protected as a computer. When used in a criminal enterprise, for example to call customers in a drug ring, accompanied by the reasonable suspicion they are being used as such, then the phones should be subject to search incident to lawful arrest. This analysis is similar to the one the Court used in Arizona v. Gant, to allow searches when the police have a reasonable suspicion that evidence relating to the arrest will be recovered in the automobile.

c. United States v. Cotterman

United States v. Cotterman196 presented the Ninth Circuit Court of Appeals with a border search of electronic equipment. While border searches are generally presumptively reasonable and require no individualized suspicion of criminal

193 Id. at 34-35

194 471 U.S. 386 (1985)
195 This was the Chief Justice Burger’s description of the vehicle in the opinion. Id. at 386.
196 Docket No. 09-10139 (March 8, 2013)(en banc)
activity, search of electronic equipment is qualitatively distinct. When Howard Cotterman entered the United States from Mexico, his two lap top computers and digital camera were taken 170 miles away and its contents searched without a warrant. Pornographic pictures of children were found. The Court, in a rehearing en banc, found that the warrantless search violated Cotterman's constitutional rights under the Fourth Amendment. The Court stated, "A person’s digital life ought not be hijacked simply by crossing a border" and imposed a reasonable suspicion standard for follow-up searches such as the one that occurred. The Ninth Circuit observed that while a suitcase provided a person with the opportunity to pack a limited amount of belongings, people can now store an extensive amount of their personal information — data like contacts, emails, text messages, photos, financial records — on portable devices like smartphones, laptops and tablets. Said the Court, "It is as if a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried." A reasonable suspicion standard for forensic searches protected travelers from a "computer strip search" every time they needed to lawfully cross the border. Interestingly, the Court found that password protection does not in and of itself give rise to reasonable suspicion, but is relevant in the totality of circumstances analysis.

3. Pluralism and Local Structures

Given the rapid development of technology devices, existing precedent provides but a rough guide to future analyses. These analyses, though, can still be predictive and general, while incorporating the understanding that circumstances, and the realities of cultural and factual realities, matter. The analyses simply would be based on the existing facts and realities created by the new data sets or technological advances. Any analysis can still be based on essential themes consistent with the text and intent of the Fourth Amendment. These themes suggest courts should consider a duality of factors: (1) the invasiveness, duration and intent of the government conduct; and (2) the nature, exposure and impact of the invasion.

197 In United States v. Ramsey, 431 U.S. 606 (1977), the Court held that international border searches are reasonable "pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."
198 Id. at ____.
199 Id. at ____.
200 Id. at ____.
201 See, e.g.,
202 By including intent, the test limits government discretion to engage in invasive tactics. Even the Third Amendment on quartering soldiers reflects that idea.
203 In light of the new realities and the stated rationales for searches incident to arrest, searches of cellular “smart” phones incident to lawful arrests generally
The requirement of at least a legitimate and articulable suspicion of criminal wrongdoing to search a cellular telephone, without any circumstantial suspicion that it would contain evidence relating to the crime is consistent with *Kyllo*, which, while concerning a house, warned against seemingly innocuous invasions revealing very personal and private information. The concept is also consistent on a broader scale with the abhorrence of writs of assistance, which are pictorially viewed as fishing expeditions – when a line is cast, it is hoped without any rhyme or reason that it hooks a fish.

*United States v. Warshak*, where the Sixth Circuit Court of Appeals recognized a right to privacy under *Katz* for email, requiring probable cause before a government could search them, is instructive.* While *Warshak* is factually distinct from cell phone searches, provides recognition of the new role data sets have in a digital society. It is not simply the aggregation of data that matters, but the way these data sets can be analyzed and then used with no expiration date. Without checks and balances, and a clear distinction between the public and private domains, the private domain would shrink to an incredibly small size.

4. Exceptions

Like almost all legal rules and principles, exceptions exist, justifying a search of a cell phone incident to a lawful arrest. Stun guns can be disguised as cell phones, and flash mobs can be arranged with the cellular phone serving as the organizing should be considered privacy encroachments, requiring some legitimate and articulable reason for the search.

*204* 631 F.3d 266 (6th Cir. 2010).

*205* The Court in *Warshak* held:

Warshak enjoyed a reasonable expectation of privacy in his emails vis-a-vis NuVox, his Internet Service Provider. *See Katz v. United States*, 389 U.S. 347 (1967). Thus, government agents violated his Fourth Amendment rights by compelling NuVox to turn over the emails without first obtaining a warrant based on probable cause. However, because the agents relied in good faith on provisions of the Stored Communications Act, the exclusionary rule does not apply in this instance. *See Illinois v. Krull*, 480 U.S. 340 (1987). *Id.* at 267.

*206* See, e.g., the film, “Honey, I Shrunk the Kids,” (IMDb 1989) for the visual equivalent.

*207* Just see all of the exceptions relating to cars, for stopping autos, to asking occupants to leave the car, to “frisks” of autos, to searches, to checkpoints and so on.

When these occur, there is ample justification to search the phone for an officer’s safety, to interdict on-going crime, or to preserve evidence.

III. Conclusion

Multi-function devices based on advancing technology have helped to create the new realities of the 21st Century, especially enhanced and altered perception. Given government-private partnerships and the routing of almost all information through third parties, an all-or-nothing definition of privacy no longer is functional. Even if once cabined by logical contours, the idea of a “reasonable expectation of privacy” is being yanked and pulled and varies depending on one’s generation, facility with technology, and understanding about existing intrusions.210 While Carney presented the Supreme Court with a 20th Century headache -- the need to classify a multi-functional device, a Recreational Vehicle, that did not fit neatly into existing categories, the cell phone provides a similar challenge in the 21st Century. Notably, the Belton-Gant line of case law was the product of advancing technology in the form of an evolving automobile. When form is separating from function as we understand it in the post-digital world, we need to apply the analysis to the new realities created by the technology, including multiple factors such as how invasive is the government’s actions, and what is the specific, articulable purpose in the invasive conduct. “Smart” phones are certainly not just phones, but they are not homes either; instead, they are best seen currently as portals into the past, present and future of their owners – a big window for rummaging around into intimate and closely held secrets. While a search incident to arrest is based on firm grounds of imminent destruction of evidence and securing the encounter for safety purposes, searching a cell phone generally does not invoke either basis for a search. While exceptions exist, the cell phone generally should not be treated like a Robinson container, an Edwards paint chip or a Chimel possession.

210 Thus, the expectations of Steve Jobs when he was running Apple Computers, for example, would have been very different than the expectations of a college student or retiree.